CLAIMS:

1. Method for authenticating a first unit to a second unit comprising the steps of:

a) exchanging authentication data between said first unit and said second unit, said authentication data being retrieved from an authorisation list comprising a list identifier, and

b) checking the authenticity of the authorisation list and the origin of the authentication data from a valid authorisation list.

2. Method according to claim 1, wherein authentication of said first unit is terminated if said step of checking fails.

3. Method according to claim 1, wherein said first unit comprises an application unit including an application and said second unit comprises a security unit.

4. Method according to claim 3, wherein said authorisation list comprises a certified application list comprising information about authorised applications.

5. Method according to claim 4, wherein in said step a) a certified public key of said application unit retrieved from said certified application list and a list identifier of said certified application list is transmitted from said application unit to said security unit, wherein in said step b) said certified public key of said application unit and said list identifier of said certified application list is checked by said security unit.

6. Method according to claim 5, further comprising the steps of

b1) transmitting a certified public key of said security unit from said security unit to said application unit, and

b2) checking said public key of said security unit by said application unit against a certified security unit revocation list.

7. Method according to claim 6, wherein said public keys are checked by use of a public key of a certification unit provided by said certification unit to said security unit and said application unit.

8. Method according to claim 5, wherein said certified application list is provided and updated by a certification unit.

9. Method according to claim 1 or 8, wherein said list identifier is distributed together with data carriers or from any of said first unit, second unit or said certification unit.

10. Method for transmitting data securely over a transmission channel from a second unit to a first unit comprising a method for authenticating said first unit to said second unit according to claim 1, further comprising the steps of:

c) encrypting data to be transmitted using an encryption key by said second unit, and

d) transmitting said encryption key and the encrypted data from said second unit to said first unit or determining said encryption key by said first and said second unit.

11. Method according to claim 10, wherein said authorisation list is distributed together with said data to be transmitted, with data carriers, with application units or applications.

12. Data transmission system for transmitting data securely over a transmission channel comprising:

a) a first unit for transmitting authentication data from said first unit to said second unit, said authentication data being retrieved from an authorisation list comprising a list identifier,

b) a second unit for checking the authenticity of the authorisation list and the origin of the authentication data from a valid authorisation list and for transmitting said data over a transmission channel from said second unit to said first unit.

13. Data transmission system according to claim 12,
wherein the second unit is provided for encrypting data to be transmitted using an encryption

key, and for transmitting said encryption key and said encrypted data from said second unit to said first unit or for determining said encryption key by said first and said second unit.

14. Data transmission system according to claim 12, further comprising a certification unit for providing a public key of said certification unit for checking said authentication data and for providing and updating said authorisation list.

15. Data transmission system according to claim 12, further comprising a computer comprising a reading unit for reading a data carrier storing the data to be transmitted, wherein said first unit is part of said computer provided for running an application and wherein said second unit is part of said computer connected to or arranged in the reading unit provided for decrypting and re-encrypting data read from said data carrier.

16. Data transmission apparatus for transmitting data securely over a transmission channel comprising:

a) a first unit for transmitting authentication data from said first unit to said second unit, said authentication data being retrieved from an authorisation list comprising a list identifier,

b) a second unit for checking the authenticity of the authorisation list and the origin of the authentication data from a valid authorisation list, for encrypting data to be transmitted using an encryption key, and for transmitting said encryption key and said encrypted data from said second unit to said first unit or for determining an encryption key by said first and said second unit.